ATTACKS ON GEOGRAPHIC ROUTING PROTOCOLS FOR WIRELESS SENSOR NETWORK

A thesis submitted in partial fulfilment of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

By

Rahul Ramteke

(Roll no. 107CS059)

Sunil Kumar Panda

(Roll no. 107CS018)

Under the guidance of :

Prof. S.K. Jena

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India

National Institute of Technology Rourkela

Certificate

This is to certify that the project entitled, **Attacks on Geographic Routing Protocol for Wireless Sensor Network** submitted by **Rahul G. Ramteke** and **Sunil Kumar Panda** is an authentic work carried out by him under my supervision and guidance for the partial fulfillment of the requirements for the award of **Bachelor of Technology Degree** in **Computer Science and Engineering** at **National Institute of Technology, Rourkela**.

To the best of my knowledge, the matter embodied in the project has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Date -9/5/2011
Rourkela

Prof. S.K. Jena
Department of Computer Science and Engineering
National Institute of Technology Rourkela

Abstract

With the increase in the military and several other applications of Wireless Sensor Network, provisions must be made for secure transmission of sensitive information throughout the network. Most of the routing protocols proposed for ad-hoc networks and sensor networks are not designed with security as a goal. Hence, many routing protocols are vulnerable to an attack by an adversary who can disrupt the network or harness valuable information from the network. Routing Protocols for wireless sensor networks are classified into three types depending on their network structure as Flat routing protocols, Hierarchical routing protocol and Geographic routing protocols. Large number of nodes in a wireless sensor network , limited battery power and their data centric nature make routing in wireless sensor network a challenging problem. We mainly concentrate on location-based or geographic routing protocol like Greedy Perimeter Stateless Routing Protocol. Sybil attack and Selective forwarding attack are the two attacks feasible in GPSR. These attacks are implemented in GPSR and their losses caused to the network are analysed.

Acknowledgement

We are overwhelmed with gratitude while availing this opportunity to express our hearty indebtedness to our guide **Prof. S.K. Jena**, Department of Computer Science and Engineering, National Institute of Technology Rourkela for rendering his invaluable guidance, motivation and encouragement for the completion of this research project.

We would sincerely like to thank **Mr. Suraj Sharma** for his constant support, inspiration and cooperation. He stood by us whenever we encountered any problem.

We would additionally like to thank the Department of Computer Science and Engineering for providing all the facilities and accessories.

Date - 9/5/2011

Rourkela

Rahul Ramteke

Sunil Kumar Panda

Contents

List of Figures

Chapter 1

Introduction

1.1 Wireless Sensor Network

Wireless Sensor Networks(WSN) is an interconnection of a large number of nodes deployed for monitoring the environment or system by means of measurement of environmental parameters like temperature, pressure, humidity. Some of the military applications of sensor networks are battle field surveillance and detection of attack by weapons of mass destruction. Sensor networks can also be effectively used for forest fire detection, flood detection, and monitoring habitats of animal's .Sensor networks are usually deployed in the conditions where continuous human intervention is not possible. Hence the set-up and maintenance of sensor networks should be autonomous. Sensor networks should also be adaptable to changing connectivity due to failure of node or introduction of new nodes. Sensor nodes being highly energy constrained pose serious challenges to the maintenance of highly scalable robust wireless network. Most of the routing protocols proposed for ad hoc networks and sensor networks are not designed with security as a goal. Hence many protocols are vulnerable to an attack by an adversary to breach the network or harness valuable information from the network.

1.2 Architecture for Nodes in Wireless Sensor Networks

The nodes have to meet the requirement of a specific application. They should be small cheap, portable and energy efficient.
The basic components of a node[12] are

- Sensor and actuator - an interface to the physical world designed to sense the environmental parameters like pressure and temperature.
- Controller - is to control different modes of operation for processing of data
- Memory - storage for programming data.
- Communication - a device like antenna for sending and receiving data over a wireless channel.
- Power Supply- supply of energy for smooth operation of a node like battery.

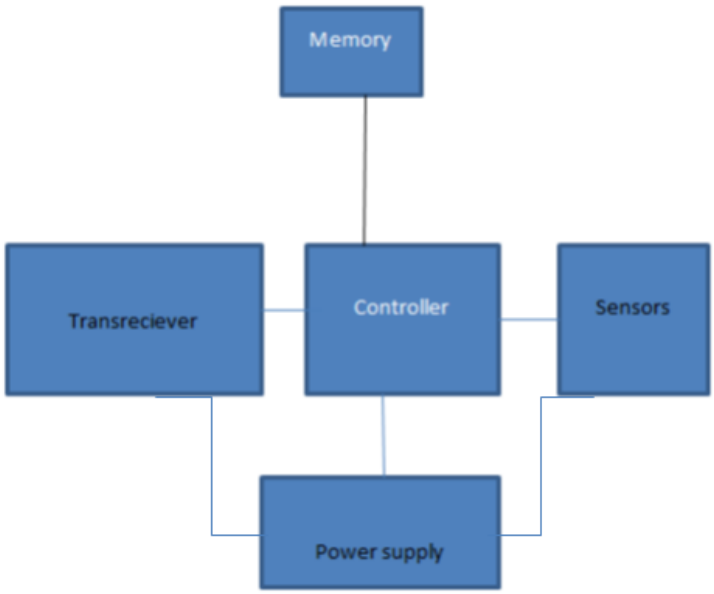

Figure 1.1: Single Node Architecture

The power supply to the node is limited .hence the design of protocols should be such that minimum energy is required for communication of information. The energy

conservation of nodes can be achieved by introducing and using multiple states of operation with reduced energy consumption in return for reduced functionality. For a controller typically three states of operations can be used active, idle and sleep .The choice of operational stage should be made on basis of time for external stimuli so that the transitions between various states should be optimal as transitions between states take time and energy.

1.3 Challenges in Routing for Wireless Sensor Networks

Low power ,limited bandwidth ,limited energy supply are main problems to be encountered in design of Wireless Sensor Networks . Main aim is to carry out data communication and prevent degradation by energy management techniques to prolong the lifetime of network.
Some routing challenges[9] are

1. Node deployment can be deterministic or randomized. In deterministic , sensor nodes are placed manually in a predefined path unlike randomized where, if the resultant distribution is not uniform, optimal clustering becomes necessary for connectivity.

2. Energy consumption without losing accuracy: In multi-hop wireless sensor network each node performs dual activity - data sender and a data router[12].The malfunctioning of some nodes due to power failure can lead to topological changes and again re-routing of packets can lead to energy and power failure and lead to energy and power loss.

3. Data reporting model: It can be event driven, query driven and time driven. Time driven is used for periodic data monitoring .Sensor switch on sensor nodes periodically and sense data and transmit the sensed data. In event driven if some drastic change in value of the sensed attribute event occurs in environment sensor nodes sense it and transmits.

4. Heterogeneity : Some sensor nodes differ in their technical design due to application orientation, data routing or communication becomes little problem due

to technical issues because sensing rate is different for different sensors.

5. Data Centricity: In Wireless Sensor Network multiple nodes are deployed to report an event for redundancy. The identity of the nodes providing data is not of much concern as compared to data supporting the occurrence of that event. Due to the presence of large number of nodes in a wireless sensor network it is not possible to assign a global identifier to each node.This networking approach is called data centric networking.

6. Scalability: A large number of sensor nodes should be deployed in sensing area. A routing scheme must be able to work with these huge number of sensor nodes. After data routing it should go to sleep state.

7. Fault tolerance: Failure of certain nodes due to power will effect the overall routing scheme. So formation of new links should be accomplished for routing of data to base stations. Re-routing of packets through network requires more energy.

8. Coverage : Wireless Sensor Networks must be deployed in a large area to ensure more accuracy of the events occurring in the environment.

1.4 Applications of Wireless Sensor Networks

Wireless Sensor Networks are used in many applications[13] such as

1. Military and civil applications such as target field imaging.

2. Weather monitoring and tactical surveillance.

3. Detecting ambient conditions such as temperature , movement, sound, light or the presence of certain objects.

4. They are used for disaster management.(Here a large number of sensor nodes are dropped from helicopter. So that it can be used for finding survivors, Identifying risk areas and making the rescue team more aware of the overall situation in the disaster area) .

1.5 Motivation and Challenges

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer application, such as industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Routing Protocols for wireless sensor networks should address challenges like lifetime maximization, robustness , fault tolerance and self-configuration properties of nodes. With wide range of applications ,designing a routing protocol that caters to the needs of wireless sensor networks as well as providing security of data have become an active research area in computer science. Integrating a new routing protocol in QualNet and simulation of attacks over GPSR and their analysis are some of the challenges encountered during the project.

1.6 Problem Statement

To implement Greedy Perimeter Stateless Routing protocol for Wireless Sensor Network, identify the attacks feasible, simulate and analyse selective forwarding attack and sybil attack over GPSR.

Chapter 2

Background

2.1 Classification of Routing Protocols

Routing protocols[9] are responsible for routing data packets from source node to the destination node. Along with routing ,the protocol aims to meet the requirements and challenges faced by the wireless sensor network. A routing protocol for wireless sensor network should be scalable for large number of nodes and exhibit characteristics like fault tolerance for reliability, energy efficiency for prolonged network lifetime and data centric.

2.1.1 Behavioural classification of Routing Protocols

Depending on the behaviour for establishment of paths from source to destination routing protocols can be classified as *proactive, reactive, hybrid*[9]. In Proactive routing protocol routes are predetermined. Reactive routing protocols are event driven the routes are determined on demand basis. Hybrid routing protocol is a combination of both reactive and proactive routing protocol to enhance network performance.

2.1.2 Network structure based Routing Protocols

Routing protocols can also be classified on the basis of network structure as Flat Network Routing, Hierarchical Network Routing and Location based routing[9].

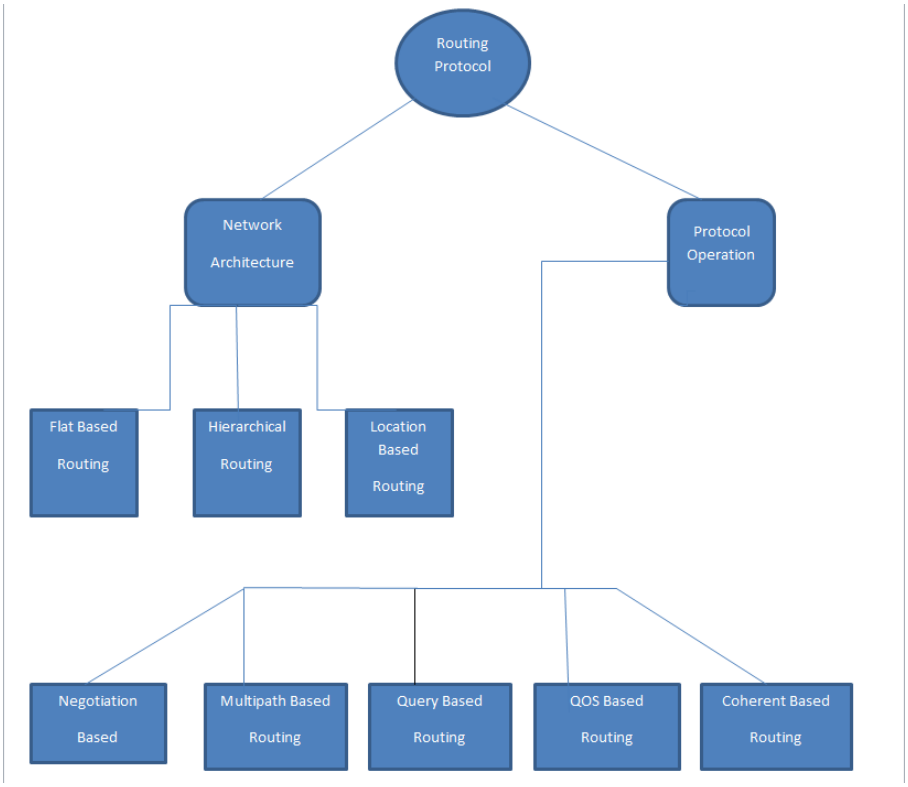

Figure 2.1: Classification of Routing Protocols

Flat Network Routing

A flat network structure is the one in which all the nodes have the same responsibility for routing of data. The contribution of nodes for routing data packets through out the network is similar. Flat routing protocols[9] are multi hop routing protocols .Due to large number of nodes in a wireless sensor network, assignment of global identifier to each node is not possible. Thus the routing should be data centric where base stations send queries to certain regions and waits for the data from the sensors deployed at selected region. Regions are areas in a network in whose vicinity some event occurs [9].

It is of various types such as

1. SPIN(Sensor Protocols for Information via Negotiation)[14]
2. Directed Diffusion[24]
3. Rumor Routing[25]
4. MCFA(Minimum Cost Forwarding Algorithm)[26]

5. Gradient Based Routing(GBR)[27]
6. COUGAR[28]
7. IDSQ(Information driven sensor querying) and CADR(Constrained Anisotropic diffusion routing)[29]
8. ACQUIRE(Active Query Forwarding In sensor Networks)[30]
9. Energy Aware Routing[31]

Hierarchical Network Routing

Hierarchical routing protocol[9] is also called as cluster based routing protocol. Initially it has been proposed for wire line networks. Hierarchical routing protocols also meet the requirement of energy efficiency in wireless sensor networks. In cluster based routing protocol high energy nodes are used for purpose such as sending and processing of data packets while low energy nodes are used for sensing of data from the target area .The process of creation of clusters and assignment of task to these cluster heads can result in scalability of overall system, prolonged lifetime, energy efficiency .Cluster based routing is used to initiate data aggregation ,reduction of data packets sent to the base station, lowering the energy consumption of nodes used in a wireless sensor network. This routing protocol consists of techniques meeting the needs of a network such as scalability[9] and efficient communication.
Hierarchical routing protocol can be of various types:

1. LEACH Protocol[14]
2. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)[15]
3. Threshold-sensitive Energy Efficient Protocols (TEEN[16] and APTEEN[17])
4. Small Minimum Energy Communication Network (MECN)[18]
5. Self Organizing Protocol (SOP)[19]
6. Sensor Aggregates Routing[20]

7. Virtual Grid Architecture routing (VGA)[21]

8. Hierarchical Power-aware Routing (HPAR)[22]

9. Two-Tier Data Dissemination (TTDD)[23]

Location based Routing

In location based routing[9] data packets are routed towards the destination by using the geographic location of nodes. Sensor nodes are addressed by means of their location. These class of routing protocols are highly scalable and energy efficient as they basically leverage on the location information of the nodes which can be easily obtained by exchanging the co-ordinates of nodes. The location of nodes may also be directly available by directly communicating with the satellite, using GPS (Global Positioning System), if nodes are equipped with a small and low power GPS receiver. The location based or geographic routing protocols can be effectively used in a wireless sensor network consisting of very large number of nodes to find the routes without much consumption of energy [9]. Thus geographic routing protocols meet the scalability and energy requirements of wireless sensor network.
Geographic routing protocols are of various types :

1. GPSR(Greedy Perimeter Stateless Routing Protocol)[1]

2. Geographic Adaptive Fidelity(GAF)[2]

3. GEAR(Geographic Energy Aware Routing)[11]

4. GOAFR(The Greedy Other Adaptive Face Routing)[3]

5. MFR, DIR and GEDIR[4]

GPSR(Greedy Perimeter Stateless Routing Protocol)

GPSR[1] is a geographic routing protocol which selects the next node which is geographically closest to the destination. This packet forwarding technique is called Greedy forwarding. This may lead to a situation when all the neighbouring nodes are away from the destination than the current node through which packet is to be

routed. Such regions in a network are called voids. The packet then needs to be routed along the perimeter of the void. This packet forwarding technique is called Perimeter forwarding. Thus, GPSR uses a combination of greedy and perimeter forwarding technique to route data towards the destination. GPSR forms the core of our research and is explained in detail in chapter 3.

Chapter 3

GPSR and feasible attacks

Greedy Perimeter Stateless Routing (GPSR)[1] is a geographic or location based routing protocol that uses the geographic positions of routers and packets destination to make packet forwarding decision.Shortest-path algorithms are state proportional to the number of hops away from destinations whereas, GPSR is a stateless protocol as it does not require the overall topology of the network to be maintained rather it depends only on local topology maintained by every node. Each node in a sensor network keeps track of the location of its immediate neighbours by using a simple beaconing algorithm. Periodically each node transmits a beacon to its immediate neighbours on the broadcast MAC address containing its own identifier and position. The inter beacon transmission interval is uniformly distributed in the interval [0.5B, 1.5B] to keep up the most current positions of the neighbours . While not receiving any beacon from a particular neighbour for longer period of time which is greater than time-out interval T, the GPSR router assumes that the neighbour has failed or gone out of range and deletes that neighbour from its table.In GPSR each node needs the propagation of topology information for all those nodes which are single hop distance. Thus the state required is minimum[1].

As the name suggests GPSR routes the data packets in greedy mode. Greedy forwarding is used throughout the network whenever possible but in the regions where greedy forwarding fails to route packet further towards the destination, the packet is temporarily transmitted in the perimeter mode.

3.1 Greedy Forwarding

To forward a packet to its neighbour a source must know the geographic location of the destination. This information can be obtained by a location server like GPS. A packet can then be routed towards the destination in the greedy mode. In a greedy mode a node selects the next node as that neighbour which is geographically closest to the destination. Thus, it selects a locally optimal node as the next hope till it can find such neighbour or until the destination is reached. Consider an example shown in Figure. 3.1 . In the given figure , $\boldsymbol{x}$ receives a packet which is to be destined[1] for $\boldsymbol{D}$. $\boldsymbol{x}$'s radio range is represented by a thin lined circle which is centred at x,and the radius of the arc is equal to the distance between $\boldsymbol{y}$ and $\boldsymbol{D}$ is shown as the thin lined arc about $\boldsymbol{D}$. Among all its neighbours $\boldsymbol{x}$ forwards packets to $\boldsymbol{y}$, because the distance between $\boldsymbol{y}$ and $\boldsymbol{D}$ is actually less than that of between $\boldsymbol{D}$ and any node of the $\boldsymbol{x}$'s neighbour[1]. Greedy forwarding has a great advantage as it rely only on knowledge

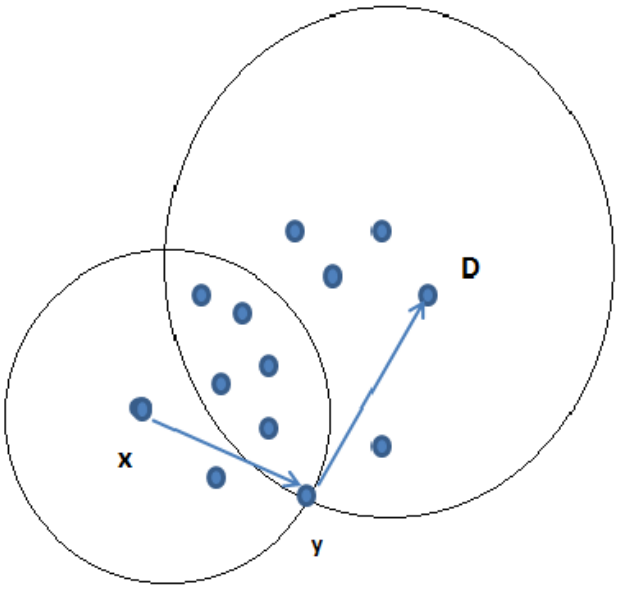

Figure 3.1: Greedy forwarding example

of the forwarding node's immediate neighbours. Thus the state required is negligible and the amount of memory and the processing in the sensor network is considerably saved. Thus GPSR[1] can save much amount of energy and can scale to large number of nodes in Wireless Sensor Network.

3.2 Perimeter Mode

The greedy forwarding technique to route using only the position of neighbour nodes comes with one limitation: there may be topologies which requires a data packet to move temporarily away from the destination. A simple example of such topology is shown in Figure 3.2. In this case, $\boldsymbol{x}$ is closer to $\boldsymbol{D}$ as compared to its neighbours

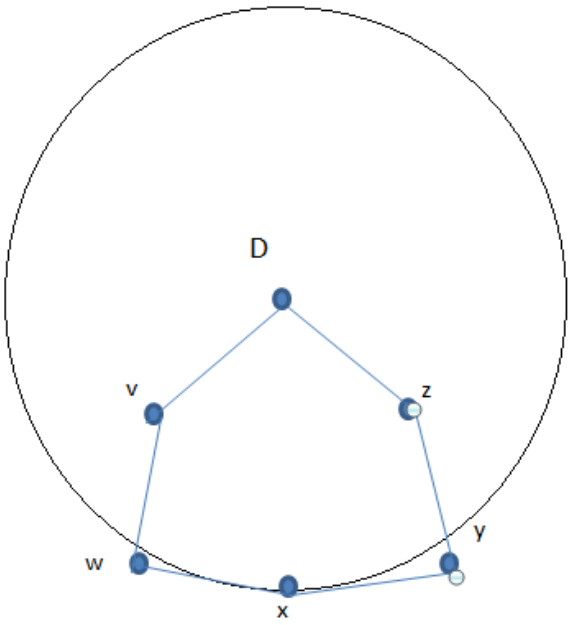

Figure 3.2: Greedy forwarding failure, $\boldsymbol{x}$ is a local minimum in its geographic proximity to $\boldsymbol{D}$,$\boldsymbol{w}$ and $\boldsymbol{y}$ are farther from $\boldsymbol{D}$

$\boldsymbol{w}$ and $\boldsymbol{y}$. Again the thin lined arc about $\boldsymbol{D}$ has a radius equal as compared to the distance between $\boldsymbol{x}$ and $\boldsymbol{D}$. Thus, there is no node neighbouring $\boldsymbol{x}$ whose distance to $\boldsymbol{D}$ is less than the distance between $\boldsymbol{x}$ and $\boldsymbol{D}$. This is represented by a void as shown in Figure.3.3. Now there exist two paths via $\boldsymbol{w}$ and via $\boldsymbol{y}$ through which $\boldsymbol{x}$ can route packet towards $\boldsymbol{D}$. Hence, $\boldsymbol{x}$ has to shift the packet temporarily away from the destination. $\boldsymbol{x}$ then selects the next node according to the right hand rule and the packet follows the path along the perimeter of the void towards the destination and the packet is said to enter into the perimeter mode[1].

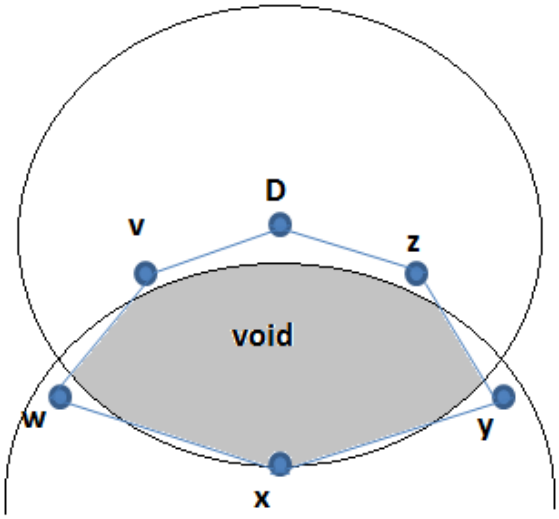

Figure 3.3: Node $\boldsymbol{x}$'s void with respect to destination $\boldsymbol{D}$

3.3 Right Hand Rule

The right hand rule in graphs is used to route the packet whenever the packet encounters a void. Thus right hand rule says that when arriving at node $\boldsymbol{x}$ from node $\boldsymbol{y}$, the next edge traversed will be the next sequential counter-clockwise about $\boldsymbol{y}$ the edge (x,y). This rule traverses the interior of a closed polygonal region in a clockwise order as shown in Figure 3.4. the triangle bounded by the edges between nodes $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$, in the order $(y \rightarrow x \rightarrow z \rightarrow y)$. This rule also traverses an exterior region, as described in this case in counter-clockwise edge order[1].

Unfortunately, the right-hand rule does not yield a traversal of the perimeter of a closed polygon on all wireless network graphs. On graphs with edges that cross, the right-hand rule may instead take a degenerate tour of edges that does not trace the boundary of a closed polygon. Such graphs with crossing edges are known as non-planar graphs. An example of a non-planar graph appears in Figure 3.5. Here, when $\boldsymbol{x}$ originates a packet to $\boldsymbol{u}$, the right-hand rule results in the tour $(x \rightarrow u \rightarrow z \rightarrow w \rightarrow u \rightarrow x)$. The no-crossing heuristic: if, during traversal of a graph by the right hand rule, the candidate next edge crosses an edge taken earlier in the traversal, that

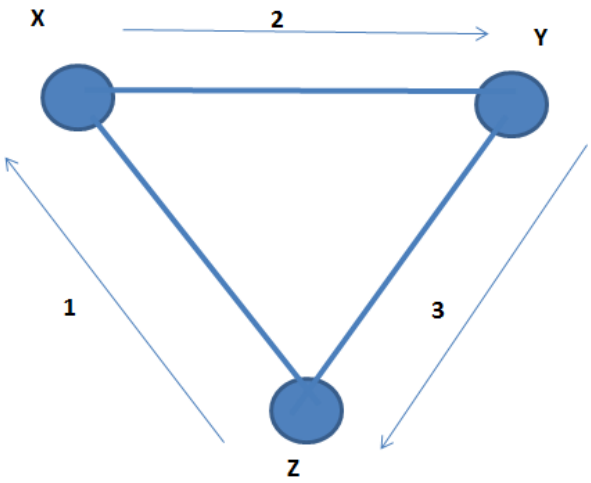

Figure 3.4: Right Hand Rule Traversal for a polygon

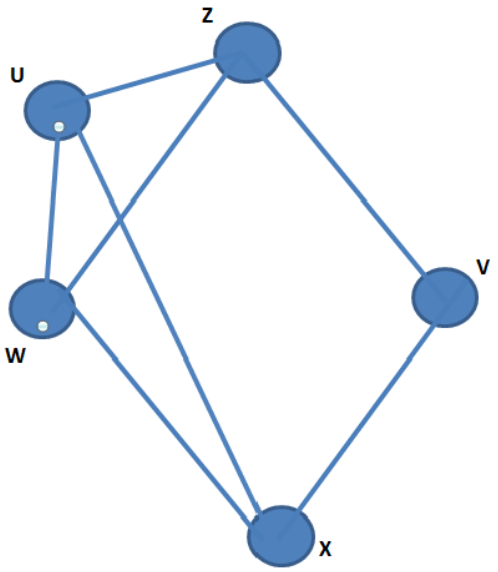

Figure 3.5: A network with crossing edges. The right-hand rule gives the tour $(x \to u \to z \to w \to u \to x)$

candidate next edge is ignored, and the next edge in counter-clockwise order is taken, instead. The purpose of this heuristic is to remove crossing edges from the graph, so that the right-hand rule takes the intended tour. In the case of Figure 3.5, starting from $\boldsymbol{x}$, after taking the path $(x \rightarrow u \rightarrow z)$, the no-crossing heuristic ignores edge (z, w) at $\boldsymbol{z}$, because it crosses the previously taken edge (x, u) the graph, the heuristic has the desired effect: the complete clockwise outer edge tour $(x \rightarrow u \rightarrow z \rightarrow v \rightarrow x)$. This heuristic traverses all the nodes along the perimeter of void and helps route packets to the destination[1].

3.4 Planarized Graphs

Planarized graphs are used to remove cross links in the network. A graph is said to be planar if no two edges cross.The Relative Neighbourhood Graph (RNG) and Gabriel Graph (GG)[1] are two long known planar graphs. The RNG or GG algorithm yields a network with no cross edges or crossing links. However for this scheme to be successful ,removal of cross edges from graph to reduce it to the RNG or GG must be done and also it must not produce disconnection in the graph, because this may lead to partitioning of the network[1].

3.4.1 Relative Neighbourhood Graph(RNG)

The RNG is defined as follows: An edge (u, v) will exist between the vertices of u and v, if the distance between $d(u, v)$ is always less than or equal to the distance between the vertex w, and whichever among u and v is farther away from v. In equational form[1]: $\forall w \neq u, v : d(u, v) < max[d(u, w), d(v, w)]$

Figure 3.6 depicts the rule for constructing RNG. The shaded region drawn between u and v, must be empty and any of presence of node w for (u, v) has to be included in the RNG. The boundary of the lune can be stated as the intersection of the circles passing about u and v of radius $d(u, v)$.

3.4.2 Gabriel Graph(GG)

The Gabrie Graph[1] is defined as follows – An edge (u,v) may exist between vertices u and v if no other vertex w is present within the circle whose diameter is uv. In

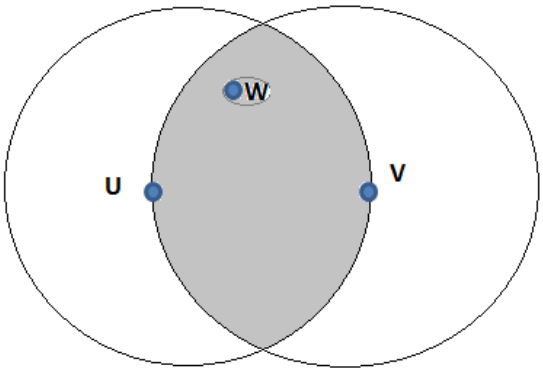

Figure 3.6: The RNG graph. for edge (u, v) to be included, the shaded lune must contain no witness w.

equational form[1]: $\forall w \neq u, v : d^2(u, v) \leq [d^2(u, w) + d^2(v, w)]$

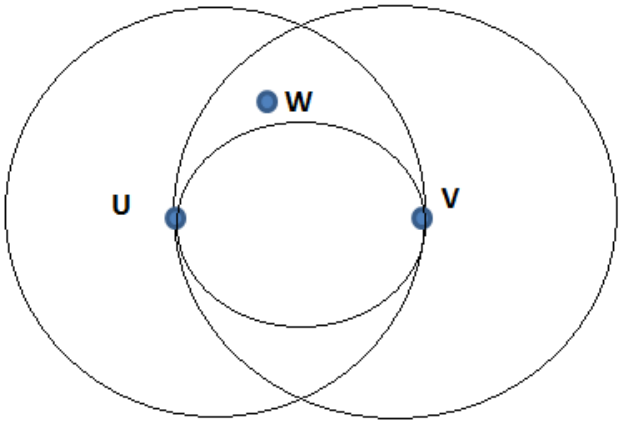

Figure 3.7: The GG graph

Figure 3.10 depicts the rule for constructing GG. As the midpoint of uv is the centre of the circle with diameter uv, a node can remove its non GG links from a full neighbourhood list N.

Both these algorithms for rendering the graph of the radio network planar take time $O(deg^2)$ at each node, where deg is the node's degree in the full radio graph. It has been shown in the literature that the RNG is a subset of the GG. This is consistent with the smaller shaded region searched for a witness in the GG, as compared with in

the RNG. Figure 3.10 shows a full unit graph corresponding to 200 nodes randomly placed on a 2000-by-2000-meter region, with radio ranges of 250 meters; the GG subset of the full graph; and the RNG subset of the full graph[1].

Figure 3.8: Left: the full graph of a radio network. 200 nodes, uniformly randomly placed on a 2000 x 2000 meter region, with a radio range of 250 m. Center: the GG subset of the full graph. Right: the RNG subset of the full and GG graphs

The full Greedy Perimeter Stateless Routing algorithm combines greedy forwarding on the full network graph with perimeter forwarding on the planarized network graph where greedy forwarding is not possible[1].

3.5 Attacks on Geographical Routing Protocols

Greedy Perimeter Stateless Routing Protocol is robust and efficient for the applications of Wireless Sensor Network but it was not designed with security as a goal. The broadcast nature of communication along with the stringent energy constraints prove maleficent for the security in wireless sensor network. The attacks in sensor networks can be mainly distinguished as outsider attacks and the insider attacks. In outsider attack the attacker has no special access to the sensor network whereas in an insider attack the attacker can access the sensor network and model an attack by using compromised node to run malicious code or by using stolen key material, code and data from legitimate nodes. GPSR, is susceptible to three major attacks[5] as described below

3.5.1 Selective Forwarding Attack

In a wireless sensor network some nodes may drop all the packets received for routing to the destination. Such malicious nodes can be easily detected and inferred as the absence of the link. So an alternate link can be found through which packets can be routed thus, keeping the loss of packets under control. A more subtle form of attack is realized when an adversary does not drop all the packets but selectively forwards few packets while dropping all the other packets. Such packet selection by an adversary is very difficult to detect and can cause considerable loss of packets in the network which may go undetected and eventually resulting in substantial loss of information. Selective forwarding[5] can cause no reporting or late reporting of an even in Wireless Sensor Network. We have simulated selective forwarding attack on GPSR for wireless sensor network and measured the loss incurred by the network.

3.5.2 Sybil Attack

Sybil attack[5] was first proposed by J. R. Douceur. In a Sybil attack[5] an adversary node presents multiple identities to other nodes in the network to use the services offered by the network. In wireless sensor network Sybil attack can greatly affect the effectiveness of the fault-tolerance schemes. Geographic routing protocols such as

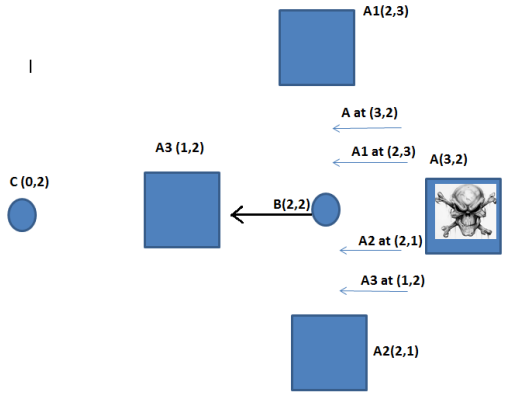

Figure 3.9: Sybil attack against geographic routing protocol

GPSR are highly susceptible to Sybil attack[5] as the identity of the nodes is related with their geographic location which can be falsely advertised. In GPSR for wireless sensor network the nodes exchange their own and also their other neighbour's location coordinates with their neighbouring nodes by sending beacons at regular intervals. An

adversary node in a network can initiate the Sybil attack by sending false location information. Thus an adversary may claim to be present at more than one location to its neighbours by sending multiple beacons, each time with a different location information as shown in Figure 3.9. Here an adversary node A, sends four different locations to node B. Thus node B is forced to send packet to node A which is actually farther from the node C to which it eventually wants to send the packet[5]. An

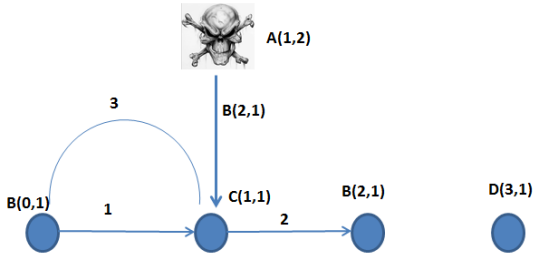

Figure 3.10: Routing loops in GPSR

adversary can also form routing loops[5] as shown in Figure 3.10 by exchanging the false location of the neighbour. As shown in Figure 3.10 an adversary node A sends false location of its neighbour B to the node C which wants to send the packet to destination D. After receiving the location of node B through A, node C sends the packet back to B as it is convinced of the location of B to be near the destination. This results into the formation of routing loops which may render the network useless by looping the packets and not routing packets to the destination. We have selected a few nods as Sybil nodes in our simulation to illustrate the effects of Sybil attack over wireless sensor network[5].

3.5.3 Spoofed or Bogus Routing

This is the most common type of attack which can take place in Geographic Routing Protocol. Main motive of this attack is to change or modify or alter the routing information which are commonly exchanged between two neighbour nodes. Thus this attack is also known as spoofed, altered or replayed routing. By spoofing or changing the routing information adversaries becomes capable of creating routing loops or it can attract network traffic or it can repel network traffic. It may extend or shorten

the routing sources or it can produce false error messages .Spoofed or bogus routing may also lead to increment of end to end latency and partitioning of network[5].

Chapter 4

Literature Survey

4.1 Defences against Sybil attacks

To defend against the Sybil attack, we would like to validate that each node identity is the only identity presented by the corresponding physical node. There are two types of ways to validate an identity. The first type is direct validation, in which a node directly tests whether another node identity is valid. The second type is indirect validation, in which nodes that have already been verified are allowed to vouch for or refute other nodes[7].

4.1.1 Radio Resource Testing

As a form of resource testing, this approach relies on the assumption that any physical device has only one radio[7]. We also assume that a radio is incapable of simultaneously sending or receiving on more than one channel. Consider that a node wants to verify that none of its neighbours are Sybil identities. It can assign each of its n neighbours a different channel to broadcast some message on. It can then choose a channel randomly on which to listen. If the neighbour that was assigned that channel is legitimate, it should hear the message. Suppose that s of the verifier's n neighbours are actually Sybil nodes. In that case, the probability of choosing to listen to a channel that is not being transmitted on, and thus detecting a Sybil node, is $\frac{s}{n}$. Conversely, the probability of not detecting a Sybil node is $\frac{n-s}{n}$. If the test is repeated for r rounds, then the chance of no Sybil nodes being detected is $(\frac{n-s}{n})^r$ Figure 5.1 shows the probability of not detecting the presence of some Sybil nodes using this method.

A more difficult case is when there are not enough channels to assign each neighbour a different channel. In this case, a node can only test some subset of its neighbours at one time. If there are$c$ channels, then the node can test c neighbours at once. Note that a malicious node not in the subset being tested can cover for a Sybil node that is being tested by transmitting on the channel that the Sybil node is supposed to be transmitting on. Suppose that in a node's set of n neighbours, there are s Sybil nodes, m malicious nodes, and g good (correct) nodes. Of these, a node can only test c neighbours at one time. Of these c neighbours, there are S Sybil nodes, M malicious nodes, and G good (correct) nodes. The probability of a Sybil node being detected[7] is then

$$\begin{aligned} Pr(detection) &= \sum_{allS,M,G} Pr(S,M,G)Pr(detection|S,M,G) \\ &= \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c} \end{aligned}$$

Now suppose that we repeat this test for r rounds, choosing a random subset to test and a random channel to listen to in each round. The probability of a Sybil node being detected[7] is then

$$\begin{aligned} Pr(detection) =& 1 - Pr(nondetection)^r_{1round} \\ =& 1 - (1 - Pr(detection)_{1round})^r \\ =& 1 - \left(1 - \sum_{allS,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c}\right)^r \end{aligned}$$

This is an effective defence against the simultaneous direct-communication variant of the Sybil attack, if the assumptions hold that an attacker cannot use one device to send on multiple channels simultaneously.

4.1.2 Random key pre distribution

Eschenauer and Gligor first proposed a random key pre distribution scheme [6]. The random key pre distribution technique allow nodes to establish a shared key with other nodes. Thus, these techniques allow nodes to establish secure links to other nodes. Random key distribution schemes can also be used to defend against the Sybil attack by node validation.

4.2 Defence against Selective forwarding attack

The multi-data flow topologies (MDT)[32] is a technique that defends against the selective forwarding attack. This technique leads to detection of selective forwarding attack as well as identification of the malicious sensor nodes. In this concept, both base station and sensor nodes share the responsibility for defending against the selective forwarding attack.

4.2.1 Multi-Data flow Topologies scheme

The MDT scheme is proposed to defend against the selective forwarding attack.The main ideas in the MDT scheme[32] can be described as follows:

- Base station divides sensor nodes into various groups before deployment.
- Each group of nodes constitutes a single data flow topology.
- Sensor nodes sent packets containing some secrets and routing information
- After deployment, multi-data flow topologies are build by sensors.
- Each sensor node belonging to one data flow topology can only communicate with the sensor nodes of the same topology
- After creation of multi-data flow topologies, each sensor node senses around itself and sends the sensed information to the base station
- WSN allows each sensor node to randomly choose the topology number.

In selective forwarding attack , malicious node drops some data packets and hence the base station does not obtain all the packets from the source node. But the Base station can recover all the lost data packets from other data flow topologies. It can be explained with an example. Suppose the whole sensing area is divided into 2 different topologies. In one topology if a malicious node exists then it will drop some packets and the base station will receive reduced number of packets , but simultaneously the base station also receives original data packets from other topologies. Hence the base station can identify the malicious node.

Locating the Faulty Sensor nodes

In wireless sensor network, the entire area is divided into smaller regions. At the time of deployment sensor are deployed in various regions. Although the base station may not be knowing the exact location of of nodes ,this concept assumes that the base station is aware of location of nodes in various regions. When the base station receives reduced number of packet from a region it marks all the nodes that region. Now base station can analyse the various regions from the data collected and can identify the malicious node.

Advantages

1. The base station receives information continuously by sensing from sensor nodes even though selective forwarding attack is active.

2. MDT scheme[32] is lightweight as well as simple too . There is no need for sensor nodes to take much effort for detection and identification of the malicious sensor nodes.

3. There is no need of resending the dropped packets after detection of malicious sensor nodes.

Disadvantages

1. The first drawback is lack of efficiency. Sensor nodes have to take much effort for detection of selective forwarding attack.

2. The second drawback is security problem. This scheme cannot detect the attack successfully in some particular condition.

3. This scheme only considers the selective forwarding attack.

4. This scheme detects some packets are dropped and identifies the possible malicious sensor nodes, the sensor node will need to obtain other routing paths to re-send the dropped packets until the base station successfully receives the packets.

Chapter 5

Simulation Results

QualNet[10] is a comprehensive suite of tools for modelling large wired and wireless networks provided by Scalable Network Technologies. It uses simulation and emulation to predict the behaviour and performance of networks to improve their design, operation and management.

Simulation Environment: QualNet
Version: 5.0.2
Tools : Matlab

We have simulated Greedy Perimeter Stateless Routing Protocol (GPSR)[8] in QualNet5.0.2. Further we have implemented Selective forwarding attack and Sybil attack over GPSR to analyse the losses incurred by the wireless sensor network. The results obtained from simulation of GPSR help us to measure the loss caused by the attacks.

5.1 Simulation of GPSR

A Wireless sensor network consisting of 17 nodes is used for simulation. Node 15 acts a source or CBR client and Node 9 acts as a destination or CBR server. All the nodes are set to use GPSR as a routing protocol. An event has occurred near node 15 which acts as a source and the event has to be reported to node 9 which acts as a base station. A sample scenario for simulation of GPSR is shown in Figure 5.1.

To find the coordinates of neighbouring nodes, each node sends beacons at regular

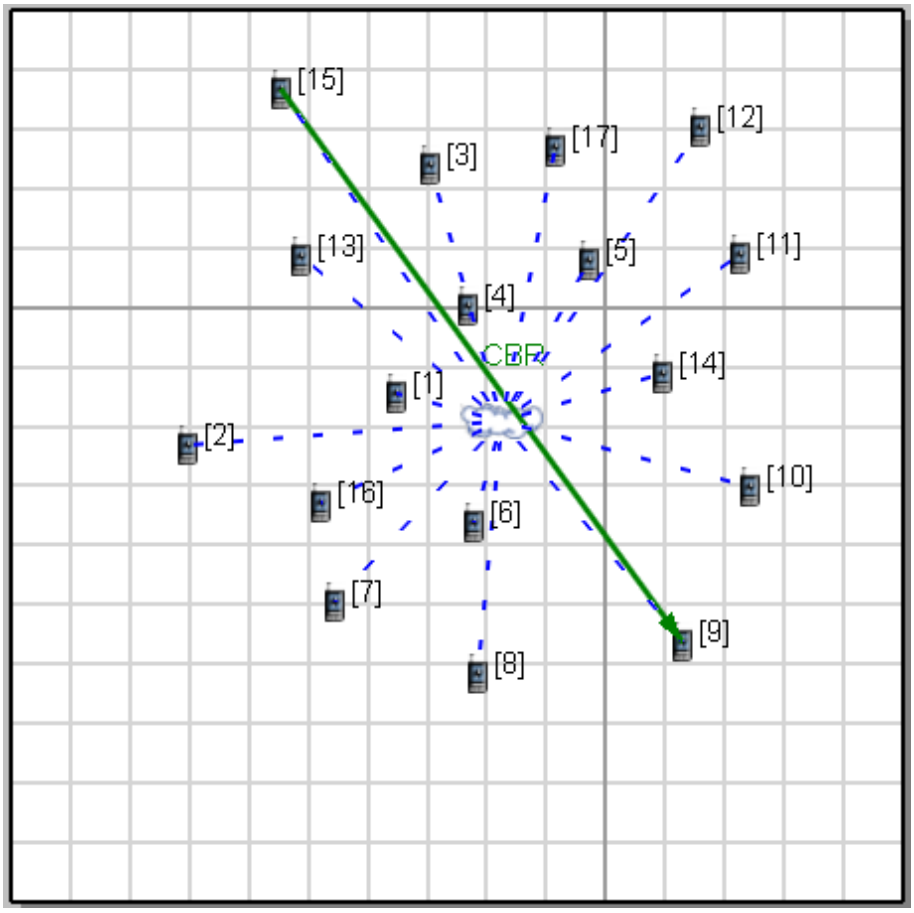

Figure 5.1: Sample scenario for GPSR

intervals. A beacon packet consists of the location of the node sending the beacon as well as their neighbours location. The total number of beacon sent during simulation by each node is 68.A node can receive beacons from more than one neighbour. Total number of beacons sent and received during simulation is shown in figure 5.2 for each node.

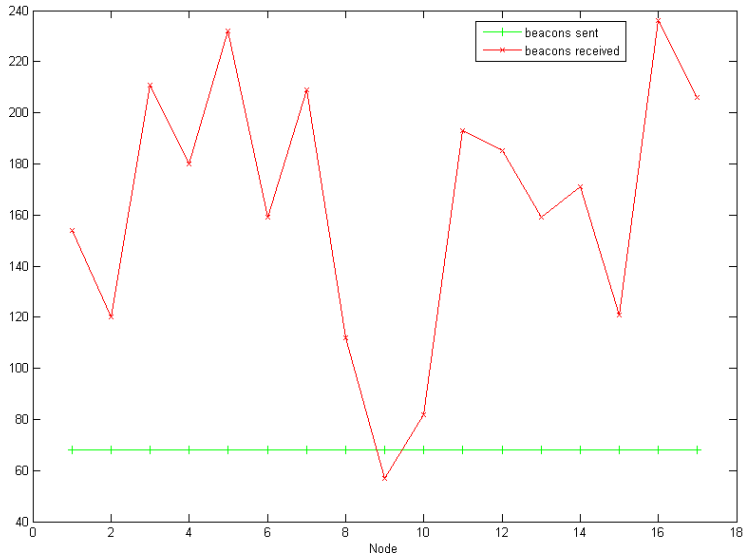

Figure 5.2: Total number of beacons sent and received

Once the location of neighbouring nodes are known packets can be routed towards the destination in greedy mode. As shown in figure 5.3 , the number of greedy forwards by nodes 2, 5, 14 and 15 are maximum as their respective neighbours are closer to the destination.

Conversely, as shown in Figure 5.4 , nodes 9,10,14 have their respective neighbours farther from the destination. Thus they have maximum perimeter forwards. Greedy forwards and perimeter forwards are the number of packets forwarded by nodes in greedy and perimeter modes respectively.

As the packets are routed towards the destination they are switched from greedy mode to perimeter mode when they encounter a void and switch back to the greedy mode after covering the void several times until destination is reached. Figure 5.5 shows the number of packets switched from greedy mode to perimeter mode whereas Figure 5.6 shows the number of packets switched back from perimeter mode to greedy mode.

In the simulation the number of packet dropped for each node is measured to be

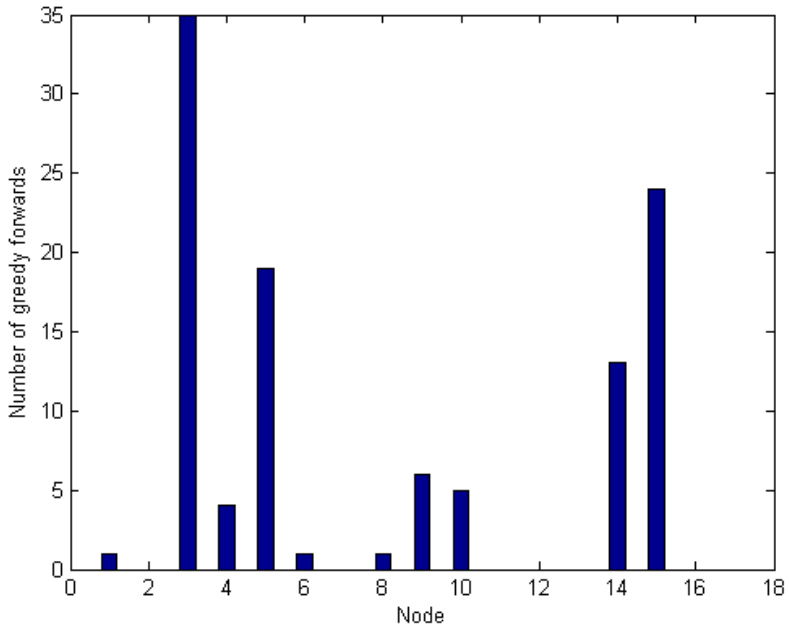

Figure 5.3: GPSR greedy forwards

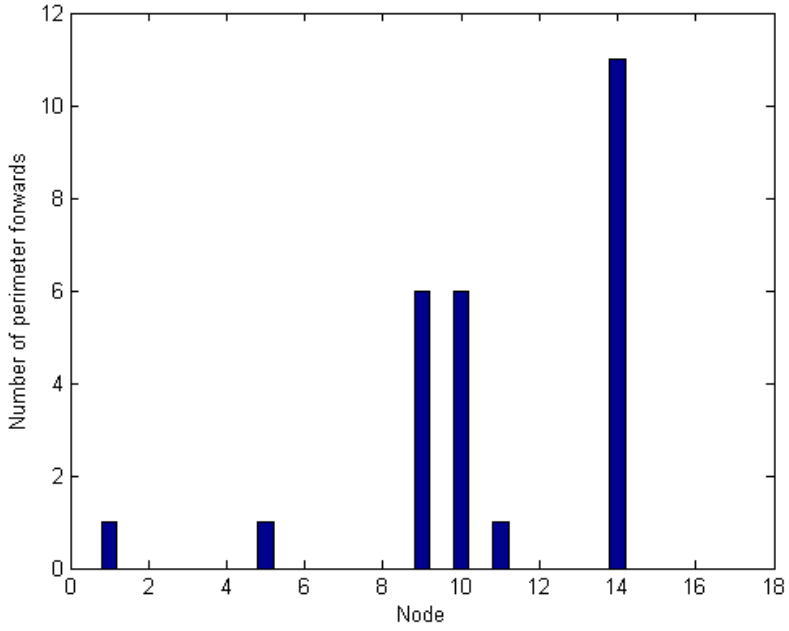

Figure 5.4: GPSR perimeter forwards

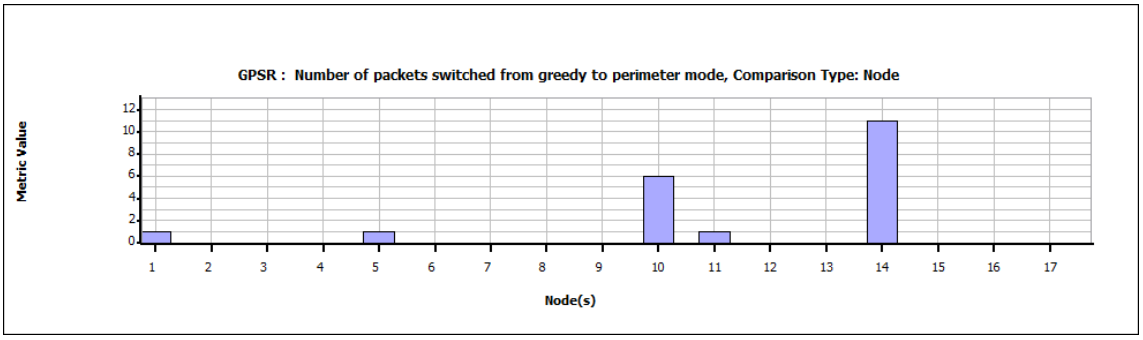

Figure 5.5: Number of packets switched from greedy to perimeter mode

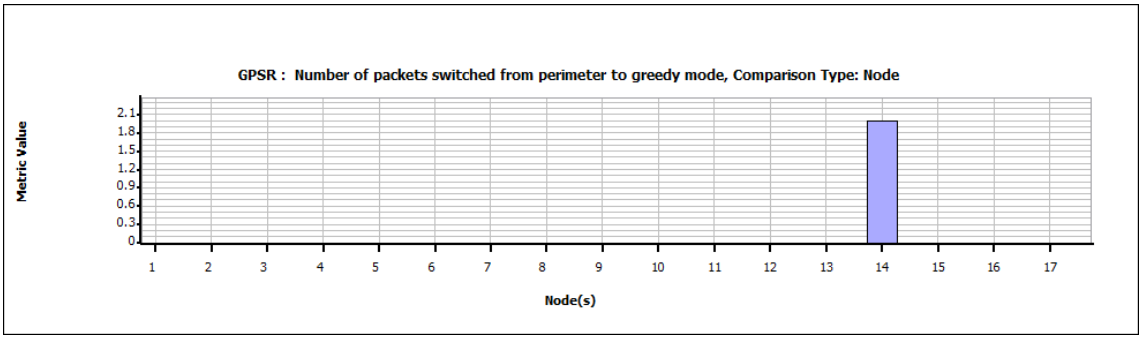

Figure 5.6: Number of packets switched from perimeter to greedy mode

zero.

5.2 Selective forwarding attack over GPSR

The example scenario of section 5.1 is used to implement selective forwarding attack over GPSR. In our sample scenario we have selected node 4,7 and 10 as malicious nodes to launch selective forwarding attack over GPSR ,as shown in Figure 5.7.

The selective forwarding attack does not alter the number of beacons sent and beacons received .Thus the total number of beacons sent and beacons received remains same as in GPSR as inferred from the figure 5.8. Similarly, selective forwarding attack does not much alter the greedy forwards and the perimeter forwards of the nodes . The smaller variation can be observed from figure 5.9, 5.10 ,5.11,5.12 which is caused to cope the number of packets lost in the routing path. The number of greedy forwards for node 11 and node 13 were 0 each in GPSR whereas in implementation of selective forwarding attack over GPSR it is found to be increased by 1 each as shown in figure 5.9.

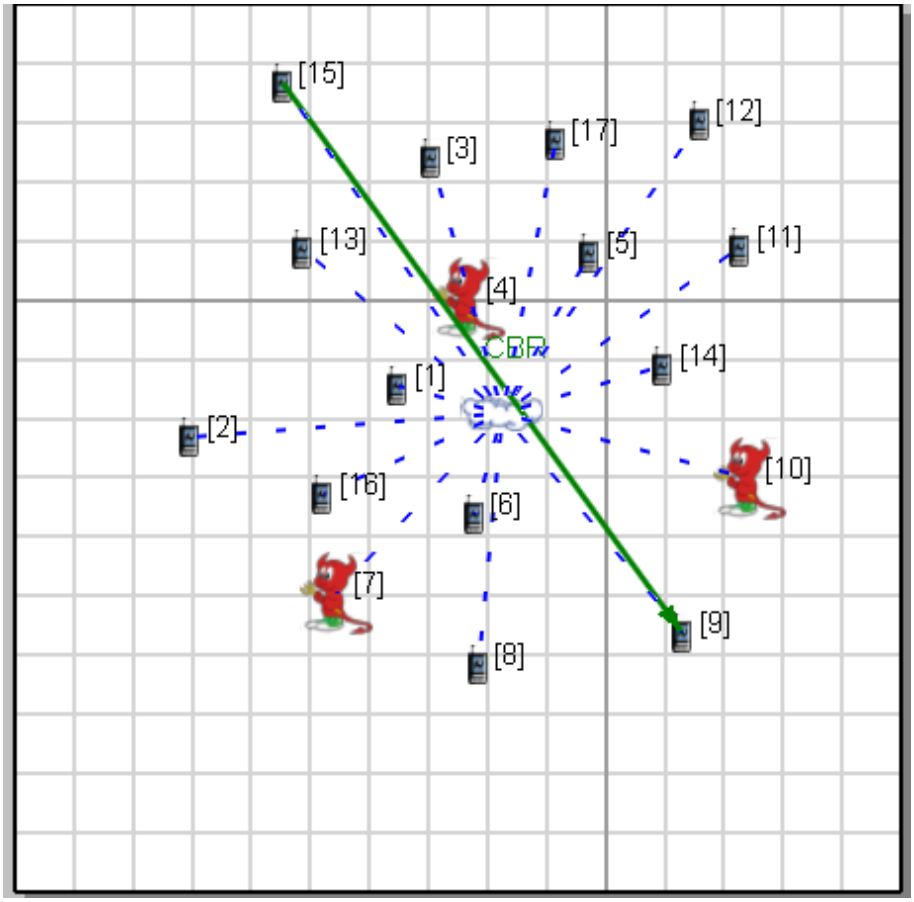

Figure 5.7: Sample scenario with Selective Forwarding Attack

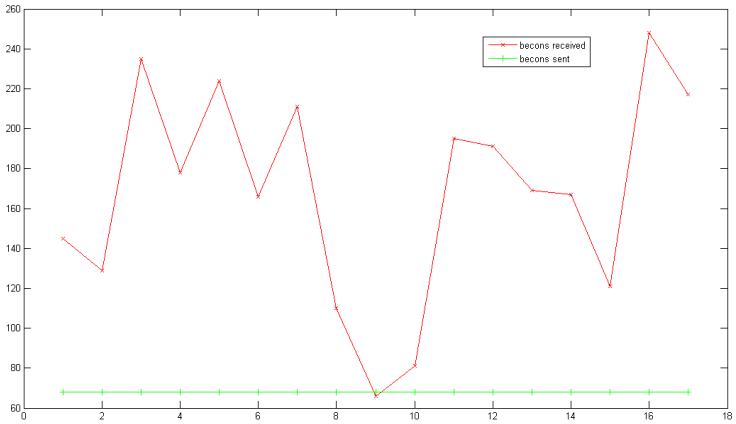

Figure 5.8: Beacon sent and Beacon received for Selective Forwarding Attack

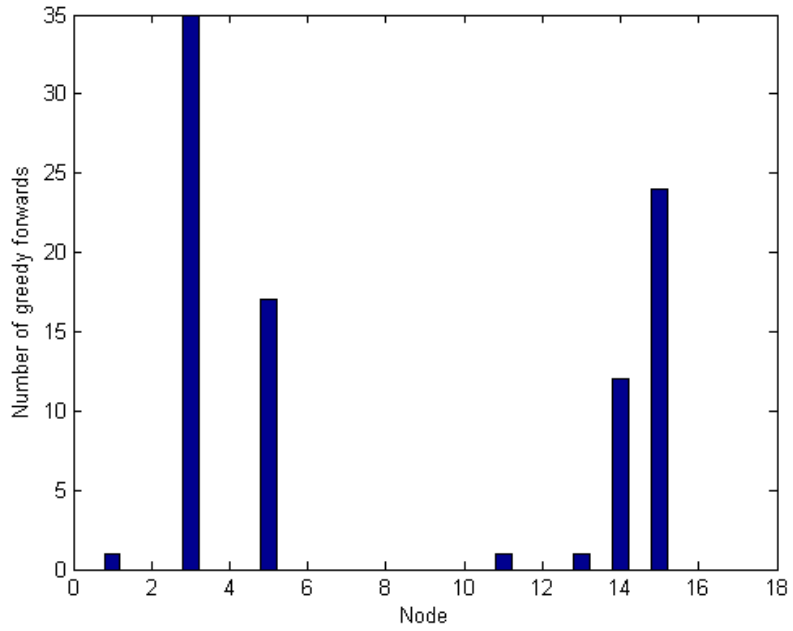

Figure 5.9: Number of greedy forwards in GPSR with Selective Forwarding Attack

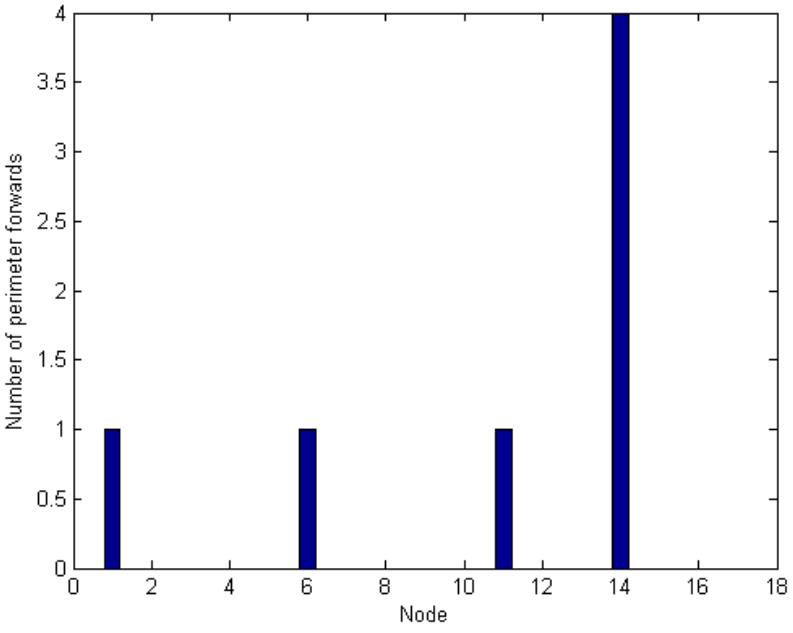

Figure 5.10: Number of perimeter forwards in GPSR with Selective Forwarding Attack

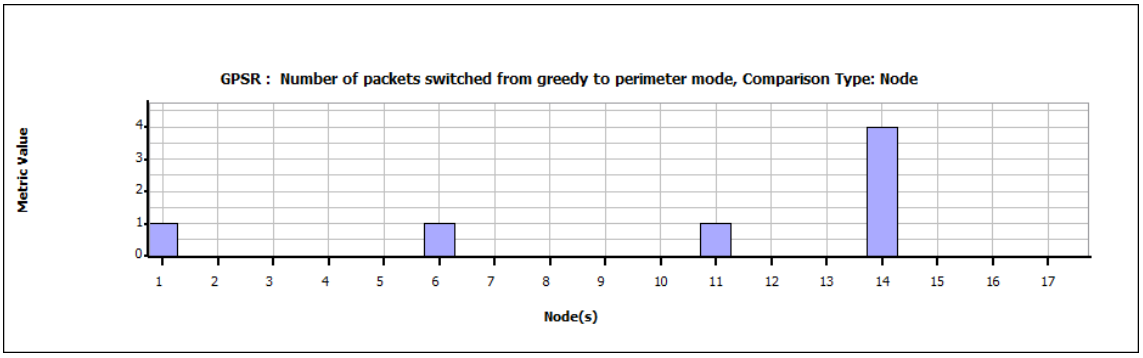

Figure 5.11: Number Of packets switched from greedy to perimeter mode in GPSR with Selective Forwarding Attack

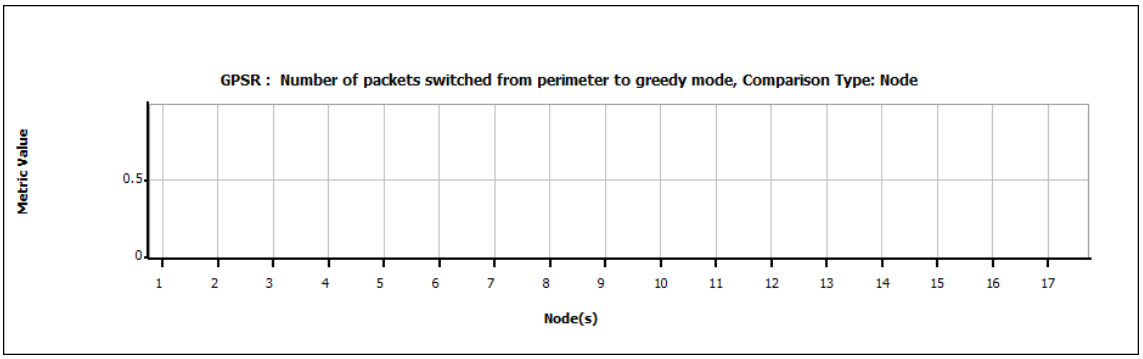

Figure 5.12: Number of packets switched from perimeter to greedy mode in GPSR with Selective Forwarding Attack

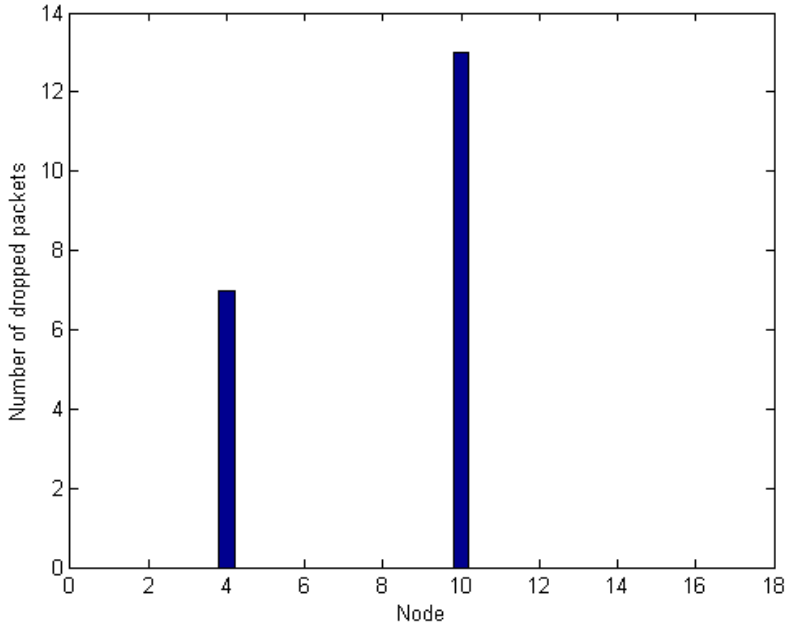

Figure 5.13: Number of dropped packets in GPSR with Selective Forwarding Attack

The malicious nodes now drop most of the packets received and selectively forward the packet. As can be seen from figure 5.13 the number of packet dropped for node 4 and node 10 is very high as compared to GPSR. Node 7 being a malicious node has zero number of packet dropped as packets are not routed through node 7. The loss of packets may lead to loss of an event being reported to the destination.

5.3 Sybil attack over GPSR

The example scenario of section 5.1 is used to implement Sybil attack over GPSR. In our sample scenario we have selected node 1, 3 and 14 as malicious nodes to launch Sybil attack over GPSR ,as shown in Figure 5.14.

Sybil attack is launched by the malicious nodes by sending more number of beacons than the normal nodes to falsely advertise multiple locations. In our case each malicious node advertises four more false locations. Thus the number of beacons sent for Sybil nodes are approximately four times the normal nodes as can be seen from Figure 5.15. This results in increase in the number of beacons received by other nodes and the number of fake identities in the network.

The Sybil attack alters the number of beacons sent and beacons received .Thus the

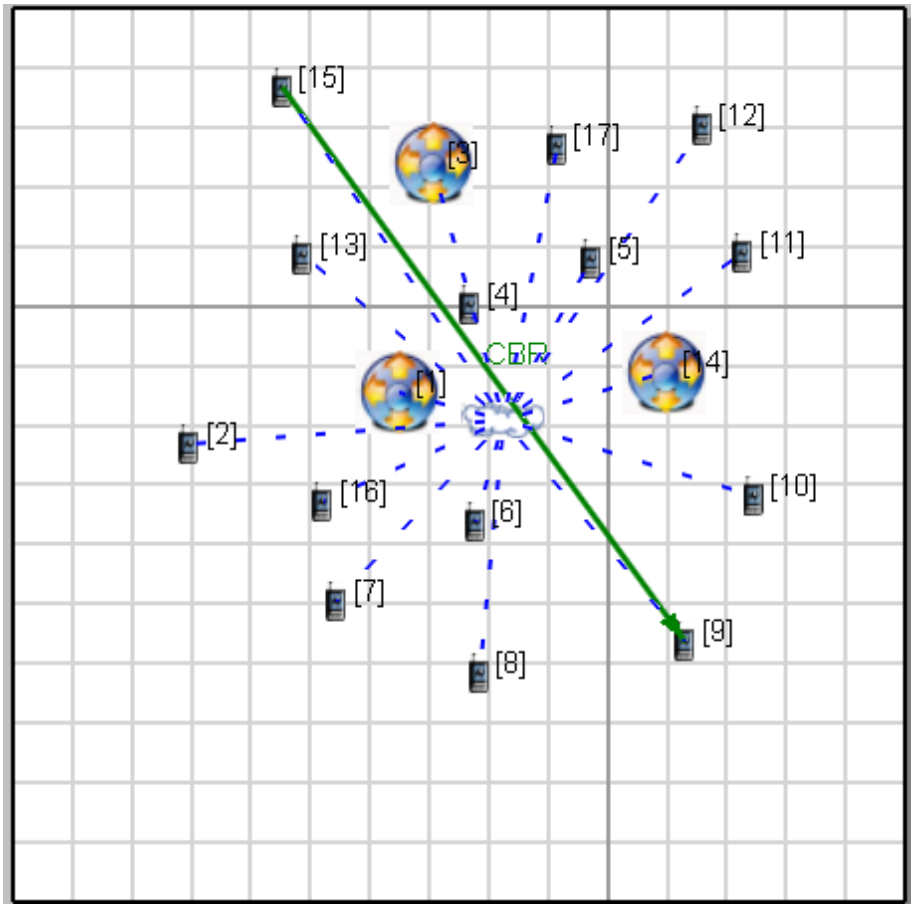

Figure 5.14: Sample scenario with Sybil attack over GPSR

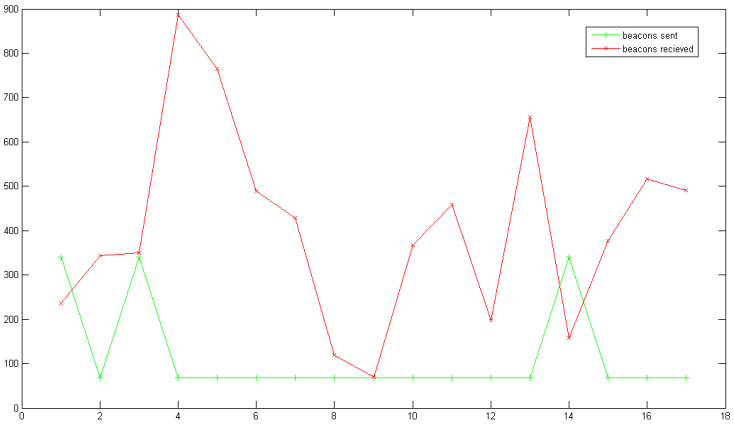

Figure 5.15: Beacon sent and Beacon received for Sybil attack over GPSR

total changed number of beacons sent and beacons received leads to small variations in network in terms of greedy forwards , perimeter forwards etc..The smaller variation can be observed from figure 5.16, 5.17 ,5.18 ,5.19 which is caused to cope the changed number of beacons and advertisement of multiple locations of a Sybil node in the routing path. The number of greedy forwards for node 8 and node 13 were 1 and 0 respectively in GPSR whereas in implementation of Sybil attack over GPSR it is found to be increased by 1 for node 13 and decreased by 1 for node 8 respectively as shown in figure 5.16.

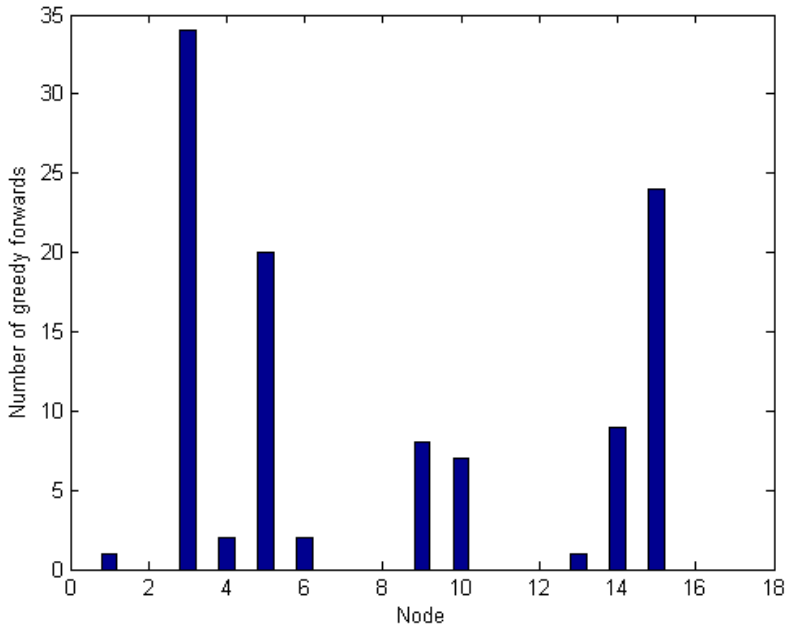

Figure 5.16: Greedy forwards for Sybil attack over GPSR

Small amount of variations can also be seen in Figure 5.17 as well as Figure 5.18 .In figure 5.17 node 5, node 11 have 0 each as perimeter forwards whereas in GPSR it has 1 as perimeter forward each for node 5, node 11. From figure 5.17 node 8 has perimeter forward increased by 1 as compared to GPSR graph. Figure 5.18 tells us that when Sybil attack is implemented in GPSR node 8 switches the data packets from greedy to perimeter mode while in GPSR simulation node 11 switched the data packets from greedy to perimeter mode in the path to the destination.

The Figure 5.19 shows that node 14 switches from perimeter to greedy mode and the number of packets it switches is 1.0 which is almost half the number of packet switched from perimeter to greedy mode by node 14 in GPSR.

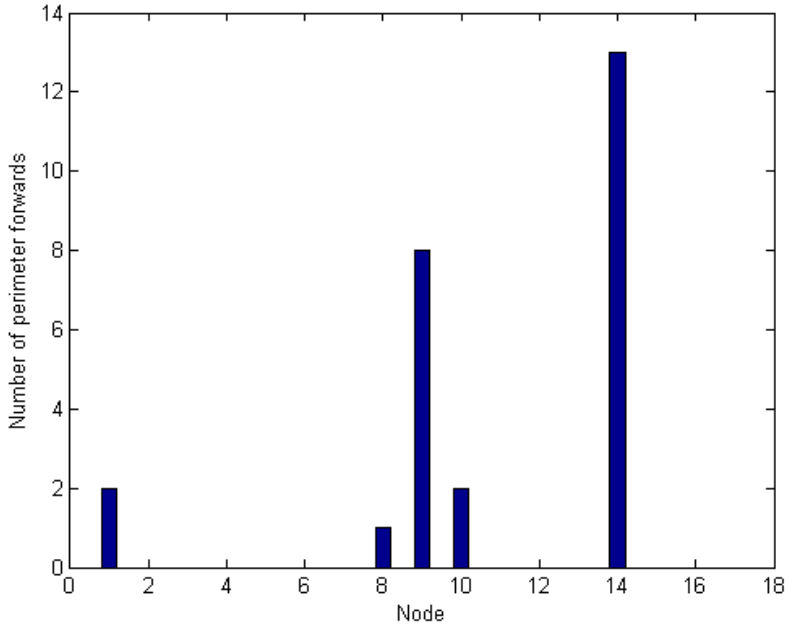

Figure 5.17: Perimeter forwards for Sybil attack over GPSR

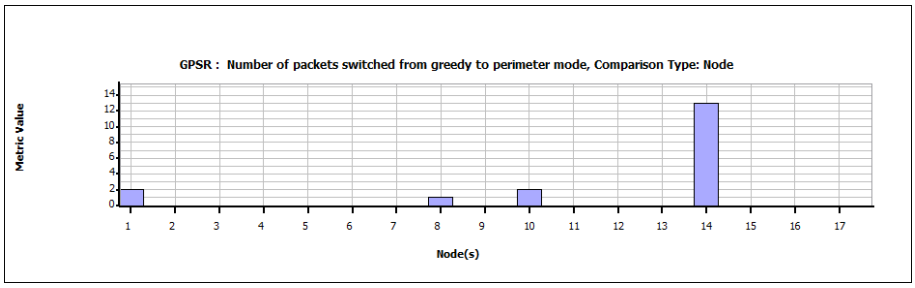

Figure 5.18: Number of packet switched from greedy to perimeter mode for Sybil attack over GPSR

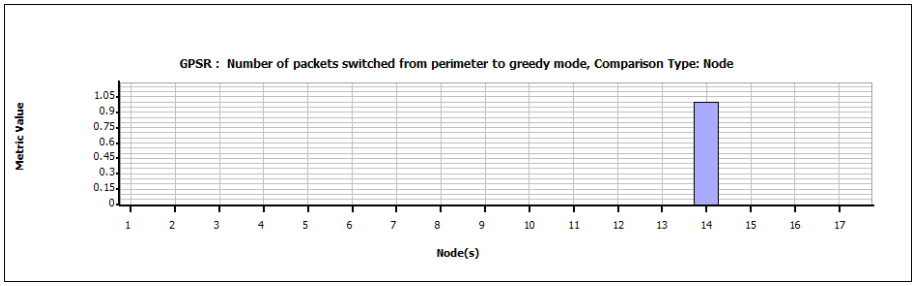

Figure 5.19: Number of packet switched from perimeter to greedy mode for Sybil attack over GPSR

The number of packet dropped by each node is zero as it was in case of GPSR.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

GPSR was simulated for wireless sensor network and the packets were found to switch from greedy mode to perimeter mode to encounter a void in the routing path.

Selective forwarding attack was simulated over GPSR and it was found that the packets dropped for malicious node has increased as compared to that in GPSR. This may lead to an event being unreported to base station.

Sybil attack was implemented and it was found that malicious node advertising multiple geographic locations sends more number of beacons to their neighbours as in comparison with GPSR , tends to alter the routes of packets and wastage of network resources.

6.2 Future Work

We look forward to design and implement a cost effective defence against Selective forwarding attack and Sybil attack over geographical routing protocol. The intended defence should be such that it uses minimum of the network resources to minimize the overhead. Our aim is to develop a countermeasure against these attacks by designing an algorithm that helps us to estimate the presence or absence of malicious node in an area of a network by using the current information about the network.

Bibliography

[1] Brad Karp and H. T. Kung. GPSR: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, New York, NY, USA, 2000. ACM.

[2] D. Estrin Y. Xu, J. Heidemann. Geography-informed energy conservation for ad-hoc routing. In *Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 70 – 84, 2001.

[3] F. Kuhn, R. Wattenhofer, and A. Zollinger. Worst-case optimal and average-case ecient geometric ad-hoc routing. In *Proceedings of the 4th ACM International Conference on Mobile Computing and Networking*, pages 267 – 278, 2003.

[4] I. Stojmenovic and X. Lin. Gedir: Loop-free location based routing in wireless networks. In *Proceedings of the Parallel and Distributed Computing and Systems*, Boston, MA, USA, Nov. 3-6 1999.

[5] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pages 113 – 127, may 2003.

[6] Haowen Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, pages 197 – 213, May 2003.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis defenses. In *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, pages 259 – 268, april 2004.

[8] UCLA Paolo Lutterotti, Giovanni Pau. Gpsr - greedy perimeter stateless routing, June 2010. contributed model.

[9] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor networks: a survey. *Wireless Communications, IEEE*, 11(6):6 – 28, dec. 2004.

[10] Scalable Network Technologies, Inc. *The qualnet 5.0.2 programming manual*.

[11] Yan Yu, Ramesh Govindan, and Deborah Estrin. Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks. Technical report, UCLA Computer Science Department, 2001.

[12] Holger Karl and Andreas Willig. *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, Ltd, 2005.

[13] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *Communications Magazine, IEEE*, 40(8):102 – 114, aug 2002.

[14] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8 - Volume 8*, HICSS '00, pages 8020–, Washington, DC, USA, 2000. IEEE Computer Society.

[15] S. Lindsey and C.S. Raghavendra. Pegasis: Power-efficient gathering in sensor information systems. In *Aerospace Conference Proceedings, 2002. IEEE*, volume 3, pages 3–1125 – 3–1130 vol.3, 2002.

[16] A. Manjeshwar and D.P. Agrawal. Teen: a routing protocol for enhanced efficiency in wireless sensor networks. In *Parallel and Distributed Processing Symposium., Proceedings 15th International*, pages 2009 –2015, apr 2001.

[17] A. Manjeshwar and D.P. Agrawal. Apteen: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In *Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, Abstracts and CD-ROM*, pages 195 –202, 2002.

[18] V. Rodoplu and T.H. Meng. Minimum energy mobile wireless networks. *Selected Areas in Communications, IEEE Journal on*, 17(8):1333 –1344, aug 1999.

[19] L. Subramanian and R.H. Katz. An architecture for building self-configurable systems. In *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on*, pages 63 –73, 2000.

[20] Qing Fang, Feng Zhao, and Leonidas Guibas. Lightweight sensing and communication protocols for target enumeration and aggregation. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '03, pages 165–176, New York, NY, USA, 2003. ACM.

[21] Ya Xu, John Heidemann, and Deborah Estrin. Geography-informed energy conservation for ad hoc routing. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, MobiCom '01, pages 70–84, New York, NY, USA, 2001. ACM.

[22] Qun Li, Javed Aslam, and Daniela Rus. Hierarchical power-aware routing in sensor networks. In *In Proceedings of the DIMACS Workshop on Pervasive Networking*, 2001.

[23] Fan Ye, Haiyun Luo, Jerry Cheng, Songwu Lu, and Lixia Zhang. A two-tier data dissemination model for large-scale wireless sensor networks. In *Proceedings of the 8th annual international conference on Mobile computing and networking*, MobiCom '02, pages 148–159, New York, NY, USA, 2002. ACM.

[24] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 56–67, New York, NY, USA, 2000. ACM.

[25] David Braginsky and Deborah Estrin. Rumor routing algorthim for sensor networks. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, WSNA '02, pages 22–31, New York, NY, USA, 2002. ACM.

[26] Fan Ye, A. Chen, Songwu Lu, and Lixia Zhang. A scalable solution to minimum cost forwarding in large sensor networks. In *Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on*, pages 304 – 309, 2001.

[27] C. Schurgers and M.B. Srivastava. Energy efficient routing in wireless sensor networks. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, volume 1, pages 357 – 361 vol.1, 2001.

[28] Yong Yao and Johannes Gehrke. The cougar approach to in-network query processing in sensor networks. *SIGMOD Record*, 31:2002, 2002.

[29] Maurice Chu, Horst Haussecker, Feng Zhao, Maurice Chu, Horst Haussecker, and Feng Zhao. Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. *International Journal of High Performance Computing Applications*, 16, 2002.

[30] N. Sadagopan, B. Krishnamachari, and A. Helmy. The acquire mechanism for efficient querying in sensor networks. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pages 149 – 155, may 2003.

[31] R.C. Shah and J.M. Rabaey. Energy aware routing for low energy ad hoc sensor networks. In *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, volume 1, pages 350 – 355 vol.1, mar 2002.

[32] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. In *TENCON 2007 - 2007 IEEE Region 10 Conference*, pages 1 –4, 30 2007-nov. 2 2007.